UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/807,607	06/01/2001	Christophe Clavier	032326-132	2078

21839 7590 11/15/2007

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER
ABRISHAMKAR, KAVEH

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
11/15/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com
debra.hawkins@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	09/807,607	CLAVIER ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 13-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 13-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

In view of the Appeal Brief filed on June 28, 2007, PROSECUTION IS HEREBY REOPENED. New grounds of rejection set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29

USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-7, 10, and 13-16 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-13 of U.S. Patent No. 7,085,378. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following mapping given below.

Application 09/807,607	U.S. Patent 7,085,378
Claim 1: A countermeasure method against attacks by differential analysis of current consumption in an electronic component using a cryptographic algorithm having a secret key, comprising the following steps: **Executing a first set of instructions in the algorithm that are critical to said attacks with a first manipulating means to deliver output data on the**	Claim 1: A countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message, of the type in which sixteen calculation rounds are employed where each round supplies an output data item is manipulated by critical instructions in at least the first three and the last three rounds, said method including the following steps:

basis of input data, and **Executing another set of said critical instructions with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data**, so that the output data and data derived from said output are unpredictable.	Forming a group comprising at least the first three rounds and another group comprising at least the last three rounds, **In each of these groups selectively applying a first sequence that uses a first manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds**, said first and second sequences being such that they supply the same result at the output from the last round in each group for the same given input message, and Selecting the sequence to be executed in the groups as a function of a statistical half probability distribution, in order to make the data manipulated by said critical instructions unpredictable. Claim 2: A countermeasure method according to claim 1, wherein each of said

	manipulating means produces output data in accordance with input data, and **wherein said other manipulating means are such that they complement at least one or both of the input and/or output data of the first manipulating means.**
Claim 2: A countermeasure method according to claim 1, wherein said first and said other manipulating means are selected for use on the basis of one-half probability statistical relationship.	Claim 1: A countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message, of the type in which sixteen calculation rounds are employed where each round supplies an output data item is manipulated by critical instructions in at least the first three and the last three rounds, said method including the following steps: Forming a group comprising at least the first three rounds and another group comprising at least the last three rounds, In each of these groups selectively applying a first sequence that uses a first

	manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds, said first and second sequences being such that they supply the same result at the output from the last round in each group for the same given input message, and **Selecting the sequence to be executed in the groups as a function of a statistical half probability distribution, in order to make the data manipulated by said critical instructions unpredictable.**
Claim 3: A countermeasure method according to claim 2, wherein said algorithm comprises sixteen computation rounds, and wherein said method comprises executing a first sequence and a second sequence,	Claim 1: A countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message, of the **type in which sixteen calculation rounds are employed where each round**

each of which is made up of at least the first three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means in at least the first round.	**supplies an output data item is manipulated by critical instructions in at least the first three and the last three rounds**, said method including the following steps: Forming a group comprising at least the first three rounds and another group comprising at least the last three rounds, **In each of these groups selectively applying a first sequence that uses a first manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds, said first and second sequences being such that they supply the same result at the output from the last round in each group for the same given input message**, and Selecting the sequence to be executed in the groups as a function of a statistical half

	probability distribution, in order to make the data manipulated by said critical instructions unpredictable.
Claim 4: A countermeasure method according to claim 3, wherein each of the first and second sequences is made up of the first three rounds.	Claim 1: A countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message, of the **type in which sixteen calculation rounds are employed where each round supplies an output data item is manipulated by critical instructions in at least the first three and the last three rounds**, said method including the following steps: **Forming a group comprising at least the first three rounds and another group comprising at least the last three rounds**, In each of these groups selectively applying a first sequence that uses a first manipulating means for said critical

	instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds, said first and second sequences being such that they supply the same result at the output from the last round in each group for the same given input message, and Selecting the sequence to be executed in the groups as a function of a statistical half probability distribution, in order to make the data manipulated by said critical instructions unpredictable.
Claim 5: A countermeasure method according to claim 3, **wherein said other manipulating means consist of second means such that, for the same input data, the complement of the output data of the first manipulating means is produced as**	Claim 2: A countermeasure method according to claim 1, **wherein each of said manipulating means produces output data in accordance with input data, and wherein said other manipulating means are such that they complement at least one or both of the input and/or output**

output data.	**data of the first manipulating means.**
Claim 6: A countermeasure method according to claim 2, **wherein said algorithm comprises executing a first sequence and a second sequence, each of which is made up of at least the three rounds, such that the order in which the sequences are executed is a function of the one-half probability statistical relationship, with the first sequence using the first manipulating means in each round, and the second sequence using the other manipulating means.**	Claim 1: A countermeasure method in an electronic component using a secret key cryptographic algorithm for calculating an encoded message from an input message, of the type in which sixteen calculation rounds are employed where each round supplies an output data item is manipulated by critical instructions in at least the first three and the last three rounds, said method including the following steps: Forming a group comprising at least the first three rounds and another group comprising at least the last three rounds, In each of these groups selectively applying a first sequence that uses a first manipulating means for said critical instructions in each round or a second sequence that uses other manipulating means for said critical instructions at least in certain rounds, said first and second

	sequences being such that they supply the same result at the output from the last round in each group for the same given input message, and **Selecting the sequence to be executed in the groups as a function of a statistical half probability distribution, in order to make the data manipulated by said critical instructions unpredictable.**
Claim 7: A countermeasure method according to claim 6, **wherein each of the first and second sequences is made up of the last three rounds, and wherein the other manipulating means used in the second sequences comprise second manipulating means and a third manipulating means.**	Claim 6: A countermeasure method according to claim 1, **wherein group is formed by the first three rounds and the last group is formed by the last three rounds.**
Claim 10: A countermeasure method according to claim 1, **wherein said**	Claim 8: A countermeasure method according to claim 1, **wherein said**

manipulating means are tables of constants.	**manipulating means are tables of constants.**
Claim 13: An electronic component which provides countermeasure against attacks on a secret key cryptographic algorithm, comprising: **A program memory having stored therein a plurality of different manipulating means for producing output data in response to input data**; A processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means; and **Means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm**,	Claim 9: An electronic security component have a countermeasure against attacks on a secret key cryptography technique in which data is manipulated by critical instructions, said component comprising: **A program memory having stored therein a plurality of manipulating means for sue during said critical instructions**, said manipulating means having complementary input and/or output data relative to one another, and **means for generating a random value that designates at least one of said manipulating means to be employed during a given execution of said cryptography technique**.

such that output data produced thereby is unpredictable.	
Claim 14: The electronic component of claim 13 wherein **said manipulating means comprise tables of constants.**	Claim 10: The electronic security component of claim 9, wherein **said plurality of manipulating means each comprise a table of constants.**
Claim 15: The electronic component of claim 13 wherein **said different manipulating means respectively produce sets of output data that are complementary to one another.**	Claim 9: An electronic security component have a countermeasure against attacks on a secret key cryptography technique in which data is manipulated by critical instructions, said component comprising: A program memory having stored therein a plurality of manipulating means for sue during said critical instructions, **said manipulating means having complementary input and/or output data relative to one another**, and means for generating a random value that designates at least one of said manipulating means to be employed during a given execution of said cryptography technique.

Claim 16: The electronic component of claim 13, **wherein said component is a smart card.**	Claim 13: The electronic security component of claim 9, **wherein said component is a chip card.**

The claims in the '607 present application are obvious in view of the claims in the Patent '378 as listed above. Both provide for manipulating means that are separate but related and produce complementary results. Furthermore, both use sixteen rounds of operations, wherein the manipulating means are tables of constants, and use a random value to select which manipulating means are to be selected. Therefore, in view of the above mappings, the claims of the present application are obvious in view of the claims of Patent '378 as given above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 13 is rejected under 35 U.S.C. 102(e) as being anticipated by Leppek (U.S. Patent 5,933,501).

Regarding claim 13, Leppek discloses:

An electronic component which provides countermeasure against attacks on a secret key cryptographic algorithm, comprising:

a program memory having stored therein a plurality of different manipulating means for producing output data in response to input data (column 1 line 63 – column 2 line 5), *wherein a encryptor operator database stores different encryptor operators*;

a processor which executes instructions in said algorithm that are critical to said attacks, in accordance with a selected one of said manipulating means (column 4, lines 24-32), *based on the address codes selected a combination of encryption operators (manipulating means) are applied to the data*; and

means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm, such that output data produced is thereby unpredictable (column 4, lines 33-38), *wherein a key (random value) is supplied to encryption assembly manager which comprises address code sequences which are used to form the combination of the encryption operators into a unique sequence (manipulating means) which is then applied to the data.*

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Leppek discloses:

The electronic component of claim 13 wherein said different manipulating means respectively produce sets of output data that are complementary to one another (column 6, lines 4-14), *wherein a complementary virtual schemes can be used.*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14, and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek (U.S. Patent 5,933,501) in view of Kocher (U.S. Patent 6,278,783).

Claim 14 is rejected as applied above in rejecting claim 13. Leppek does not explicitly teach wherein said manipulating means are a table of constants. Kocher discloses that manipulating means are constants tables (column 7, lines 15-65). Kocher teaches the uses of tables to manipulate data. These tables are filled with parameters (constants) that are updated so that attackers cannot obtain the contents of the table by an analysis of measurements. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use the tables of constants to minimize information leakage when using an electronic component such as a smart card (Kocher: Abstract).

Claim 16 is rejected as applied above in rejecting claim 13. Leppek does not explicitly disclose that the electronic component is a smart card. Kocher teaches the use of smart cards in preventing leakage of information (Kocher: see Abstract). Leppek

teaches that the information is sent from a user workstation over a network (Leppek: column 1, lines 31-38). It would have been obvious to implement the system of Leppek on a smart card because smart cards are portable.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA 11/12/07

KA
11/12/2007